



HOMELAND SECURITY PROGRAM

Project supported by a RAND Investment in People and Ideas

THE ARTS
CHILD POLICY
CIVIL JUSTICE
EDUCATION
ENERGY AND ENVIRONMENT
HEALTH AND HEALTH CARE
INTERNATIONAL AFFAIRS
NATIONAL SECURITY
POPULATION AND AGING
PUBLIC SAFETY
SCIENCE AND TECHNOLOGY
SUBSTANCE ABUSE
TERRORISM AND
HOMELAND SECURITY
TRANSPORTATION AND
INFRASTRUCTURE
WORKFORCE AND WORKPLACE

This PDF document was made available from www.rand.org as a public service of the RAND Corporation.

[Jump down to document](#) ▼

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world.

Support RAND

[Purchase this document](#)

[Browse Books & Publications](#)

[Make a charitable contribution](#)

For More Information

Visit RAND at www.rand.org

Explore the [RAND Homeland Security Program](#)

View [document details](#)

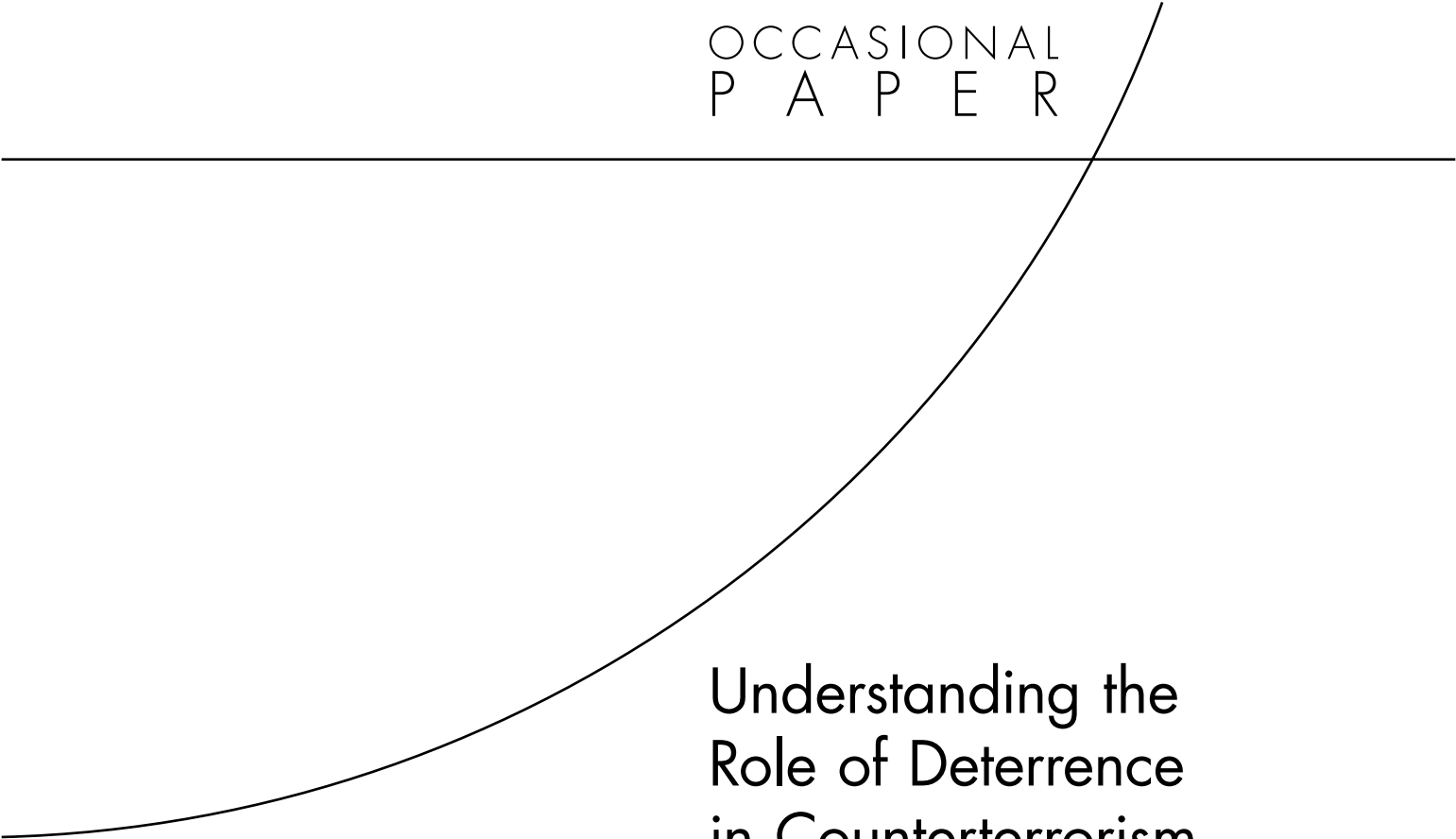
Limited Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law as indicated in a notice appearing later in this work. This electronic representation of RAND intellectual property is provided for non-commercial use only. Unauthorized posting of RAND PDFs to a non-RAND Web site is prohibited. RAND PDFs are protected under copyright law. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use. For information on reprint and linking permissions, please see [RAND Permissions](#).

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 01 NOV 2009		2. REPORT TYPE		3. DATES COVERED 00-00-2009 to 00-00-2009	
4. TITLE AND SUBTITLE Understanding the Role of Deterrence in Counterterrorism Security				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Rand Corporation,Santa Monica,CA				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 44	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

This product is part of the RAND Corporation occasional paper series. RAND occasional papers may include an informed perspective on a timely policy issue, a discussion of new research methodologies, essays, a paper presented at a conference, a conference summary, or a summary of work in progress. All RAND occasional papers undergo rigorous peer review to ensure that they meet high standards for research quality and objectivity.

OCCASIONAL
P A P E R



Understanding the Role of Deterrence in Counterterrorism Security

Andrew R. Morral, Brian A. Jackson



HOMELAND SECURITY PROGRAM

Project supported by a RAND Investment in People and Ideas

This Occasional Paper results from the RAND Corporation's continuing program of self-initiated research. Support for such research is provided, in part, by the generosity of RAND's donors and by the fees earned on client-funded research.

Library of Congress Cataloging-in-Publication Data

Morral, Andrew R.

Understanding the role of deterrence in counterterrorism security / Andrew R. Morral, Brian A. Jackson.

p. cm.

Includes bibliographical references.

ISBN 978-0-8330-4914-8 (pbk. : alk. paper)

1. Deterrence (Strategy) 2. Terrorism—Prevention. 3. National security. I. Jackson, Brian A., 1972–

II. Title.

U162.6.M6726 2009

363.325'17—dc22

2009047042

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

RAND® is a registered trademark.

© Copyright 2009 RAND Corporation

Permission is given to duplicate this document for personal use only, as long as it is unaltered and complete. Copies may not be duplicated for commercial purposes. Unauthorized posting of RAND documents to a non-RAND Web site is prohibited. RAND documents are protected under copyright law. For information on reprint and linking permissions, please visit the RAND permissions page (<http://www.rand.org/publications/permissions.html>).

Published 2009 by the RAND Corporation

1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138

1200 South Hayes Street, Arlington, VA 22202-5050

4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665

RAND URL: <http://www.rand.org>

To order RAND documents or to obtain additional information, contact

Distribution Services: Telephone: (310) 451-7002;

Fax: (310) 451-6915; Email: order@rand.org

Preface

This paper is one in the series *New Ideas in Homeland Security*, a set of RAND Corporation research papers on fundamental questions of homeland security in the United States. The series began during the transition between presidential administrations in 2008–2009, a period when approaches to homeland security were being reassessed. Each paper explores different approaches to ongoing homeland security policy problems. In doing so, they frame the kinds of questions that must be considered if policies shaping homeland security are to be effective. Questions in this area include the following: Are current practices the best and most economical ones for keeping the United States safe? Are better means available for evaluating what may work or not and why?

This series is designed to focus on a small set of policy areas, produce essays exploring different approaches to ongoing policy problems, and frame questions that need to be answered if homeland security policy is to be improved. The resulting discussions should be of interest to homeland security policymakers at the federal, state, and local levels and to members of the public interested in homeland security and counterterrorism.

This paper offers a framework for understanding how security systems may deter or merely displace attacks and how to establish the relative deterrent value of alternative security systems. Because deterrence may be the most important effect of some counterterrorism security programs, this framework may be useful to security policymakers who are trying to improve the security benefits they can achieve with limited resources.

Earlier papers in this series include:

- Brian A. Jackson, *The Problem of Measuring Emergency Preparedness: The Need for Assessing 'Response Reliability' as Part of Homeland Security Planning*, Santa Monica, Calif.: RAND Corporation, OP-234-RC, 2009.
- C. Richard Neu, *Is It Time to Rethink U.S. Entry and Exit Processes?* Santa Monica, Calif.: RAND Corporation, OP-235-RC, 2009.
- Brian A. Jackson, *Marrying Prevention and Resiliency: Balancing Approaches to an Uncertain Terrorist Threat*, Santa Monica, Calif.: RAND Corporation, OP-236-RC, 2009.
- Brian A. Jackson and David R. Frelinger, *Emerging Threats and Security Planning: How Should We Decide What Hypothetical Threats to Worry About?* Santa Monica, Calif.: RAND Corporation, OP-256-RC, 2009.
- Brian A. Jackson and David R. Frelinger, *Understanding Why Terrorist Operations Succeed or Fail*, Santa Monica, Calif.: RAND Corporation, OP-257-RC, 2009.

This effort is built on a broad foundation of RAND homeland security research and analysis carried out both before and since the founding of the Department of Homeland Security. Examples of those studies include:

- Brian A. Jackson, Peter Chalk, Kim Cragin, Bruce Newsome, John V. Parachini, William Rosenau, Erin M. Simpson, Melanie W. Sisson, and Donald Temple, *Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies*, Santa Monica, Calif.: RAND Corporation, MG-481-DHS, 2007.
- Tom LaTourrette, David R. Howell, David E. Mosher, and John MacDonald, *Reducing Terrorism Risk at Shopping Centers: An Analysis of Potential Security Options*, Santa Monica, Calif.: RAND Corporation, TR-401, 2006.
- Henry H. Willis, Andrew R. Morral, Terrence K. Kelly, and Jamison Jo Medby, *Estimating Terrorism Risk*, Santa Monica, Calif.: RAND Corporation, MG-388-RC, 2005.
- Jeremy M. Wilson, Brian A. Jackson, Mel Eisman, Paul Steinberg, and K. Jack Riley, *Securing America's Passenger-Rail Systems*, Santa Monica, Calif.: RAND Corporation, MG-705-NIJ, 2007.

The RAND Homeland Security Program

This research was conducted under the auspices of the Homeland Security Program within RAND Infrastructure, Safety, and Environment (ISE). The mission of RAND Infrastructure, Safety, and Environment is to improve the development, operation, use, and protection of society's essential physical assets and natural resources and to enhance the related social assets of safety and security of individuals in transit and in their workplaces and communities. Homeland Security Program research supports the Department of Homeland Security and other agencies charged with preventing and mitigating the effects of terrorist activity within U.S. borders. Projects address critical infrastructure protection, emergency management, terrorism risk management, border control, first responders and preparedness, domestic threat assessments, domestic intelligence, and workforce and training. Information about the Homeland Security Program is available online (<http://www.rand.org/ise/security/>). Inquiries about homeland security research projects should be sent to the following address:

Andrew Morral, Director
Homeland Security Program, ISE
RAND Corporation
1200 South Hayes Street
Arlington, VA 22202-5050
703-413-1100, x5119
Andrew_Morral@rand.org

This Occasional Paper results from the RAND Corporation's continuing program of self-initiated research. Support for such research is provided, in part, by the generosity of RAND's donors and by the fees earned on client-funded research.

Contents

Preface	iii
Figures	vii
Summary	ix
 Understanding the Role of Deterrence in Counterterrorism Security	1
Terrorist Decisions—The Targets of Deterrence	2
Security Effects on Terrorist Attack Planning	6
Raising the Costs of an Operation (Increasing an Attacker’s Expected Disutilities)	6
Lowering the Expected Payoff of an Operation	9
Increasing Uncertainties Involved in Operation Payoffs and Costs	10
Exchanging the Relative Expected Utilities of Alternative Operations	14
Strategic, Operational, and Tactical Deterrence-by-Denial	15
Strategic Deterrence	15
Operational Deterrence	16
Tactical Deterrence	17
Analyzing the Deterrent Effects of Security Measures	19
Discussion	24
 Bibliography	29

Figures

1. Model Decision Calculus for a Terrorist Attack	4
2. Candidate Deterrence-Level Analyzer	22
3. Notional Classification of the Relative Deterrent Value of Various Air-Transportation Counterterrorism Security Systems.....	24

Summary

Deterrence—a central feature of counterterrorism security systems and a major factor in the cost-effectiveness of many security programs—is not well understood or measured. This paper builds on a growing literature examining terrorist decisionmaking to examine the role of deterrence in counterterrorism strategy for homeland security. It discusses deterrence at the strategic, operational, and tactical levels and considers adaptations that would-be attackers are likely to make in response to security efforts. It also explores the connection between deterrence and risk transfer, which is the possibility that successful deterrence may result in increased danger to other targets, including those of higher value to the defender.

This paper offers a conceptual model for understanding how security systems may deter (or merely displace) attacks and a measurement framework for establishing the relative deterrent value of alternative security systems. Because deterrence may be the most important effect of some counterterrorism security programs, this framework may be useful to security policymakers who are trying to increase the security benefits they can achieve with limited resources.

Understanding the Role of Deterrence in Counterterrorism Security

Deterrence is a central concept in counterterrorism security, yet it is not well understood or measured. Without effective deterrence, counterterrorism security may simply be impractical, as noted by the Transportation Research Board (2002, p. 34): “[T]he impracticality of eliminating all transportation vulnerabilities means that efforts to deter must be a key part of transportation security strategies.” Deterrence is also a major factor in the cost-effectiveness of many security programs. For instance, even if a radiation-detection system at ports never actually encounters weapon material, if it deters would-be attackers from trying to smuggle such material into the country, it could easily be cost-effective even if associated program costs are very high. On the other hand, if smugglers can merely shift their operations to smaller ports or land routes, then the benefits of the program may be slight in spite of its narrow deterrent effect. Indeed, a recent National Research Council (2009) review of one such port radiation-detection program, the Advanced Spectroscopic Portal program, recommended that development of the program be discontinued until questions about deterrent effects, deflection (or risk-shifting) effects, and related factors central to cost-effectiveness are better understood.

This paper builds on a growing literature examining terrorist decisionmaking to examine the role of deterrence in counterterrorism strategy for homeland security. It discusses deterrence at the strategic, operational, and tactical levels and considers adaptations that would-be attackers are likely to make in response to U.S. security efforts. It also discusses the related and nettlesome connection between deterrence and risk transfer, including the possibility that some successful deterrent actions can increase the level of danger. The paper then suggests a simple analytic framework for evaluating the relative value of deterrent actions. Such a framework is necessary for ensuring that counterterrorism security investments are efficient and effective.

Prior studies and observation of terrorist-group behavior make it clear that terrorists respond dynamically to the security measures they encounter or suspect they will encounter (Jackson et al., 2007). Therefore, to optimize security strategies, the United States needs to understand how such strategies are likely to affect terrorists’ decisions about whether and what to attack (Jackson, 2009a; 2009b). Ideally, deterrence and risk-displacement effects are “designed in” so that security measures manipulate terrorist decisionmaking in ways that produce net security benefits. We explore this possibility by building on an economics literature that began with Becker’s 1968 analysis of crime and its management and has more recently been extended to investigate terrorist and security-manager decisionmaking, often in the context of economic game theory.

In the next sections, we propose a general conceptual model for how security measures affect terrorists who plan attacks. We discuss this model’s implications for understanding both deterrence and the risk-displacement effects of security measures, as well as for counterterrorist

security planning more generally. Finally, we propose a framework for evaluating alternative security measures that takes into account the possibility that deterrence merely results in risk displacement.

Terrorist Decisions—The Targets of Deterrence

Despite occasional uncertainty and periodic controversy on the point, it is by now conventional to assume that terrorists pursue their objectives rationally. Although determined terrorists—both as *individuals* and *organizations*—may be willing to risk everything to achieve their objectives, they do not wish to waste their own lives or other resources on missions that are doomed to fail or unlikely to achieve their intended results. This insight has led to a growing game-theory literature examining how to optimize security investments given the assumption that terrorists are guided by principles of expected utility theory (e.g., Bier, 2005; Golany et al., 2009; Lakdawalla and Zanjani, 2005; Major, 2002; Phillips, 2009; Zhuang and Bier, 2007, 2009; Zhuang, Bier, and Alagoz, 2009).

The distinction between terrorists as individuals and terrorist groups as organizations is important for understanding the deterrent effects of security measures. The example of individual suicide terrorists is often invoked to illustrate why security measures that threaten the safety of operatives may have less of a deterrent effect than those aimed against criminals or other attackers who want to live to see another day. Even if an individual suicide terrorist is prepared to die for a minor victory, however, this may not be true for the organization that dispatches the operative. Both may be sensitive to measures that affect the successful outcome of the operation, but the group might also be sensitive to measures that both threaten the life of the operative and provide security forces with information that could compromise the group. In our discussion, we chiefly focus on deterring organizations. From this perspective, individuals are deterred when their actions would produce unacceptable harm to their organizations. See Radlauer (2006) for a discussion of the two different targets of deterrence.

Examples of terrorists' sensitivity to operational risks abound. Hoffman (1997), for instance, quotes George Habash of the Popular Front for the Liberation of Palestine as saying, "The main point is to select targets where success is 100% assured." Although hyperbolic, the quote illustrates sensitivity to risks. In the doctrine of groups like the Provisional Irish Republican Army, requirements for operational planning include explicit consideration of how pre-attack surveillance can be used to manage and reduce operational risks. Similarly, in a document captured from the Islamic State of Iraq/al Qaeda in Iraq (Combating Terrorism Center at West Point, 2008, p. 6), a group member laments the deleterious effects on potential suicide bombers when they suspect that poor planning may result in their lives being wasted on low-value targets:

The brother . . . starts hearing stories and episodes of previous suicide bombers who carried out their attacks in the air or against walls. He hears also that the brothers will be sending him to an easy target that can be dealt with by a security or military operation. One of the brothers will inform the suicide bomber that the target will be against two police cars or one of the apostate leaders; as result [sic], his morale will deteriorate as he was hoping to cause huge damage to the apostate group, and devilish thoughts and depression crawls [sic] to his heart. The problem will increase when he hears about more suicide bombers who were

captured while carrying out their operations, since the car did not explode or as a result of failure of the booby trapped vehicle.

Rapid changes in terrorist tactics in response to effective security countermeasures—such as the decline in aircraft hijacking attempts after magnetometers were introduced as a routine part of passenger screening or a group’s decision to use indirect weapons, such as mortars and rockets, to attack targets protected by security barriers—also implicitly demonstrate terrorists’ sensitivity and rational adaptation to operational risks posed by security measures (Enders and Sandler, 2002; Jackson et al., 2007).

Because terrorists are sensitive to the risk posed by their operations but also highly motivated to achieve operational objectives or the intended payoff, they must at least implicitly undertake a kind of cost-benefit analysis of the available alternative operations. Indeed, explicit prescriptions for this sort of rational decisionmaking can be found in contemporary writings by al Qaeda strategists. For example, in *The Management of Savagery*, Naji (2006, p. 107) directs planners to weigh the “benefit and harm” of different actions they might undertake, directly echoing this sort of cost-benefit thinking. Other groups have made similar statements, either with respect to individual acts or to violent action overall. The previously cited document captured from the Islamic State of Iraq/al Qaeda in Iraq parallels this argument while criticizing some of the group’s midlevel emirs for not performing such analyses appropriately and therefore wasting operatives and resources in attacks that failed to properly weigh operational risks against probability of success (Combating Terrorism Center at West Point, 2008). In this case, risky actions are seen by the perpetrators themselves as taken not “irrationally” but out of incompetence.

For a terrorist planning an attack, different types of costs and benefits need to be considered. By thinking about how defensive measures might affect the decisions of terrorist organizations—potentially resulting in deterrence or risk displacement—we may be able to anticipate their cost-benefit calculation.

To illustrate, consider a simple bombing attack. On the benefit side, the bomb will produce immediate damage and casualties that the terrorist hopes will translate into media attention, fear among or coercive power over its target populations or states, and some longer-term progress toward achieving his or her goals. Yet, even with meticulous planning and preparation, a planner seeking to predict the magnitude of expected benefits for most operations will face considerable uncertainty. Even for something as tangible as the number of people his or her bomb will kill, the actual outcome of an operation can range from nothing (e.g., if the bomb fails or explodes at the wrong time) to the maximum number of casualties a device of its size and characteristics could produce (Phillips, 2009). On the cost side, there are predictable costs (e.g., the resources to build the bomb and stage the attack) and less-predictable ones (e.g., threats to operational security, dangers associated with handling explosives, and uncertainties in how counterterrorism response after the attack might affect the group).

The uncertainties facing the terrorist decisionmaker are important to understanding the deterrent effect of security systems, but they are rarely treated explicitly in game-theoretic analyses of terrorist decisionmaking. For example, in many analyses, terrorists are presumed to have perfect information about their probabilities of succeeding against security measures of known effectiveness. Notable exceptions we identified were Dutter and Seliktar (2007), who address uncertainty in their theoretical discussion of terrorism deterrence; Sandler, Tschirhart, and Cauley (1983), who include outcome uncertainty for the terrorist as an element of a game-

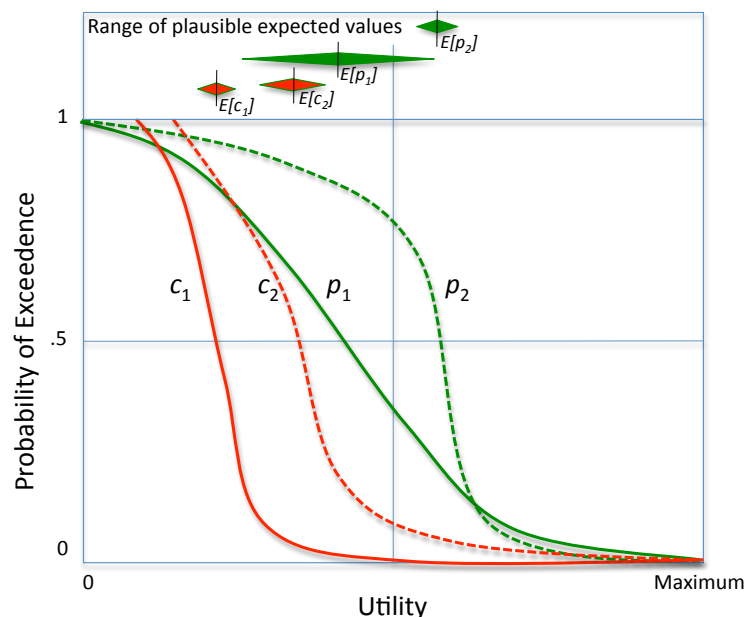
theoretic examination of the setting of demands in terrorist negotiation; and Anthony (2003), whose consideration of terrorist uncertainty about defensive measures—and steps attackers might take to reduce that uncertainty—is central to his discussion of the effectiveness of deterrence. Recent work by Zhuang and colleagues (Zhuang and Bier, 2009; Zhuang, Bier, and Alagoz, 2009) has included the topics of uncertainty and incomplete information, but these treatments have focused on deception and secrecy—i.e., uncertainty intentionally created by security actors—rather than the inherent uncertainties faced by terrorist decisionmakers.

To represent the choices before the terrorist decisionmaker, Figure 1 presents “exceedance curves” for two terrorist operations, Op 1 and Op 2. The curves illustrate the uncertainties faced by operational planners in terms of their perceived probabilities of payoffs (p) and costs (c) of each operation, both expressed in terms of the utility (or, in the case of costs, disutility) the terrorist organization can expect from undertaking either operation. Specifically, exceedance curves illustrate the probability that the payoffs (or costs) of the operation will exceed some level of utility (or disutility) for the group. Such curves make it easy to demonstrate how uncertainties faced by planners can affect their decisions.

First, note the following about the curves labeled p_1 (the possible payoffs of Op 1) and c_1 (the possible costs of Op 1):

- The payoff exceedance curve intersects the vertical axis at 1, meaning that there is a 100-percent chance of achieving at least nothing. Moving to the right, the curve has a pretty constant slope (although it is a little flatter at the beginning); this shows that the attack has a high probability of achieving at least a modest utility for the group. The curve crosses the 50-percent-chance line before hitting the midpoint of the utility range, meaning that the attack has better than a 50-percent chance of achieving less than this mid-range payoff. Thus, for an operation run by this group, there is a reasonably good chance something will be achieved, but there is a much lower chance for a large payoff.

Figure 1
Model Decision Calculus for a Terrorist Attack



- The cost curve for this operation has less uncertainty for the planner. It does not intersect the axis at 0 disutility because the group must invest some resources to stage the attack—those fixed costs are certain. The chance that the attack will produce larger levels of disutility for the group falls off quickly and reaches 0 before the midpoint of the possible range of utilities.

Op 1 represents a relatively easy choice for a terrorist decisionmaker. Although there is a chance that the attack could produce very large benefits (curve $p1$ reaches the far right of the graph), there is little chance that the costs to the group will be excessive. Although the uncertainty range around the expected utility of staging the operation is wide ($E[p1]$ at the top of the graph), it comes nowhere near the expected disutility and its associated error bar ($E[c1]$).¹ Because the expected payoff exceeds the expected costs, the operation merits consideration.

Examining both operations on the graph illustrates how a decisionmaker might choose between two attacks. In this example, Op 2 has a very high probability of achieving at least low to medium utility for the group, but the chance that it will achieve greater utilities diminishes rapidly. Op 1 has an excellent chance of achieving at least a low utility for the group, but the chances that it will achieve better utilities than will Op 2 are much lower, at least until the possibility of very high utilities are considered. At that point, Op 1 has a slightly better, although still quite low, probability of exceeding utilities of this magnitude. Op 1 is likely to cost less than Op 2, but its expected utility, $E[p1]$, is substantially lower than that of Op 2, $E[p2]$, and there is much greater uncertainty in the level of utility the group will derive from Op 1, a fact represented by the wide error bands around the expected utilities. Although the net expected utilities of both operations are positive (i.e., $E[p] - E[c] > 0$), there is nevertheless considerable uncertainty about what the true net utilities will be.

Op 1 and Op 2 could differ in terms of their targets, attack methods, levels of effort or resources devoted to attacks using similar methods, timing, and many other such factors. For example, Op 1 could be a timer-detonated improvised explosive device, whereas Op 2 could be a suicide bomber. The suicide bomber can intelligently target a group of people, so he or she has a higher probability of achieving a relatively high payoff. The suicide bomber is more costly, however, in terms of the direct costs (the life of the bomber and payments to his or her family), the risks to operational security, and attendant disutilities involved in recruiting and managing the suicide bomber, his or her family, and others who become aware of the operation.

By placing the likely payoffs and costs to the terrorist group on the same utility scale, we mean to emphasize the trade-off faced by terrorist planners. Materiel, personnel, time, and other operational costs impose disutilities on the organization that could threaten to overwhelm the benefits any operation is designed to achieve. Importantly, however, individual terrorist organizations will evaluate these utilities and disutilities differently, depending on their values, beliefs, experiences, resources, and motives. Organizations rich in expendable person-

¹ The curves in Figure 1 also enable demonstration of a much harder situation for a terrorist decisionmaker. Consider an operation whose possible payoff is represented by $p1$ but whose costs are represented by $c2$. In this case, if one considers only expected utilities, running this attack appears to be in the group's interest because $E[p1] > E[c2]$ (see the points on the horizontal lines at the top of the figure). However, this comparison shows the potentially definitive effect of cost and payoff uncertainty on the terrorist decisionmaker—the error bars associated with those expected utility estimates *overlap*. For this operation, there is a chance that the payoff that is achieved (i.e., the outcomes falling in the left-most portion of the error bar) will not, in fact, be greater than the operation's costs (if the actual outcome falls in the right-most portion of the error bar).

nel, or terrorists motivated more by the promise of rewards in the hereafter, may regard the loss of their operational team as a lesser disutility than those with fewer resources or those motivated more by earthly rewards. Similarly, mass-casualty attacks on military bases or subways might be viewed as producing very different payoff exceedance curves for different groups, depending on how those groups value the targeting of innocent civilians or the economy.

The preferences of different terrorist groups also likely lead to different strategies for achieving their objectives. Whereas some may wish to maximize their net expected utilities ($E[p] - E[c]$), others might be more cautious, adopting a strategy of minimizing the risk of low or negative net utilities, the commonly preferred “minimax” strategy described in game theory (Major, 2002). Minimally, however, it is safe to assume that planners wish to ensure that an operation’s disutilities (direct and other costs, risks to the survival of the group, etc.) do not exceed the utility of the operation from the terrorist planner’s perspective.

Security Effects on Terrorist Attack Planning

In criminology literature, deterrence is thought to be driven primarily by the likelihood and severity of punishment expected for committing a crime (Cook, 1980). Although both the likelihood and the severity of punishment surely play some role in the decisionmaking of terrorists, there are important differences between the objectives of terrorist organizations and individual criminals. For instance, most criminal activity has the objective (or hope) of avoiding accountability for the crime. The same may not be true for many terrorist acts. Thus, the criminal caught after stealing jewels or killing an enemy has failed in what he or she is trying to do, which is to perpetrate the crime and get away with it. The terrorist may be satisfied with overcoming security countermeasures and executing the attack effectively, and have little regard for his or her fate afterward and only modest concern about the consequences to his or her organization. Indeed, as long as the utility of the operation is great enough to the terrorist group, the threat of significant punishment as a deterrent may count for little. Given these differences between ordinary crime and terrorism, we suggest focusing on the potential effects of security measures on terrorist organizations and their objectives rather than on the usual assumptions about how individuals might be deterred from committing crimes.

Nevertheless, even if terrorist planners are only concerned that the costs of an operation not exceed its utility, security can be used to manipulate the operational planning of terrorists. Specifically, security can be designed to increase a terrorist’s views of expected disutilities ($E[c]$), lower their estimates of expected utilities ($E[p]$), increase uncertainty in expected utilities or disutilities, or exchange the net expected utilities of different operations. That is, programs have a deterrent effect chiefly through their effects on terrorist views of utilities, disutilities, and uncertainty. To the extent that defenses do not affect terrorist views, they will not deter terrorism even if they have an instrumental effect on the terrorists’ likelihood of succeeding.

We now consider strategies for influencing terrorists’ views of each of the key decision factors.

Raising the Costs of an Operation (Increasing an Attacker’s Expected Disutilities)

The costs of a terrorist operation include (1) the materiel, time, personnel, and other resources required to plan and execute the operation and adapt to its subsequent consequences for the group and (2) opportunity costs (i.e., the forgone benefits that could otherwise be obtained by

investing the same resources in alternative activities, including different terrorist operations or even legal activities advancing the group's goals.

Driving Up the Cost of Operations. The cost of an operation includes direct costs in terms of time, money, and the lives of suicide attackers (or other likely fatalities) as well as the cost of unplanned personnel losses, such as those that result from accidents in handling explosives or when individuals are captured in the act when an operation is disrupted. Possible expected disutilities might also include unintended political or reputational effects. Security and counterterrorism efforts could aim to increase the costs of carrying out the operation, or they could be designed to impose costs on the group as a punishment for staging the operation.

Classic deterrence-by-punishment approaches are essentially designed to affect the perceived cost of an operation (see, for example, Schelling, 1960; Long, 2008, and references therein). The early Cold War concept of deterrence rested on persuading enemies that U.S. retaliation against any attack would be sufficiently certain and severe to make the cost of attacks appear unacceptably high. Later, a stronger version of deterrence sought to assure that the would-be attackers, using their own perceptions and values, would not see a way to “win” even if they were willing to tolerate enormous costs. This version combined deterrence-by-punishment with broad deterrence-by-denial, a form of deterrence in which operations are discouraged because the expectable payoffs or success rates appear too low. During a period in which the risk of global conflict of sufficient proportions to threaten the survival of the human race was real and immediate, the mutual deterrence that large nuclear arsenals created helped ensure that nuclear warfare between superpowers never happened. In contrast, strategic-level deterrence-by-punishment may be of limited value against terrorist groups that have little infrastructure of their own to protect against attack, who may well be prepared to lose it all in the service of achieving a significant blow against the United States, and who may be harder to identify and locate after an attack than were the United States' Cold War adversaries (Davis and Jenkins, 2002; Helfstein et al., 2009).

Indeed, throughout the history of terrorism, some terrorist organizations have even acted in an attempt to *attract* such punishment, hoping that the reaction of potentially sympathetic countries or populations to that retaliation would help the terrorists advance their goals (National Research Council, 2002). As a result, it is reasonable to be skeptical about claims that deterrence through punishment is likely to be effective for most terrorist groups or could result in a stable mutual inaction between terrorist groups and the states they target in the same way that such threats produced stability between the United States and the Soviet Union during the Cold War.

Moreover, retaliatory actions available to U.S. security planners may be too modest to substantially increase the costs terrorist planners must consider. For example, arrests made in response to international terrorism by the Palestine Liberation Organization (PLO) had relatively minor effects, leading Le Vine and Salert (1996) to suggest that

since only small numbers of people were ever committed to overseas terrorism, this means that even if governments did manage to arrest or kill all of those who engaged in such acts—a feat that would demand huge resources and may well have been impossible—the leaders of the component organizations might well have decided that the casualty rate still fell within acceptable limits.

Although traditional deterrence by punishment may be of limited utility for most terrorist planners, the threat of punishment may be able to shape the behavior of others and affect terrorist behavior indirectly. For example, as Davis and Jenkins (2002) note, even if al Qaeda *in total* is unlikely to be deterred by the threat of unbearable consequences, it may be that enough component organizations and groups within or associated with al Qaeda can be deterred through targeted threats of negative consequences. If the capabilities and activities of attack planners within the group depend on tolerance or assistance from those organizations or groups, deterring them could disable the group and thereby effectively deter al Qaeda itself. For other arguments in favor of deterrence-by-punishment, see Trager and Zagorcheva (2005–2006), Bowen (2004), and Almog (2004–2005).

Swift and severe punishment is not the only way to increase the cost of terrorist operations, however. For instance, the United States pursues programs to make unconventional-weapon materials more scarce than they might otherwise be, thus increasing the expense and danger to obtain them and thereby driving up material costs. Nonproliferation programs employing former weapon scientists were designed to increase the difficulty and cost of purchasing such expertise. Interventions in other illicit-weapon markets and regulatory controls on explosives have analogous effects for familiar weapons (Hope, 2006; Boyne, 2006). Effective border and immigration controls could increase the costs of positioning attackers in the United States, if, for instance, they forced operational planners to recruit personnel who would not be identified through terrorist watch lists. Other interventions could make it more difficult for attackers to gather the information they require to plan operations, therefore requiring that they spend more time on or involve more people in operational preparation.²

Driving Up Opportunity Costs. Like all decisionmakers, terrorists must consider the opportunity costs associated with their choices. Resources devoted to one type of attack cannot also be used to carry out a different activity. In addition to trade-offs between different attack options, broader sets of opportunity costs might be considered when the terrorist organization's aims could be pursued through legal as well as terrorist action (Frey and Luechinger, 2003). Throughout the history of modern terrorism, a variety of groups have had political wings that engaged in legal activities alongside the violent or military actions taken by the group. For other groups, such activities as the provision of social services to their support communities have become an important component of the organizations' efforts to maintain their support base and pursue their broader goals.

Resources a group devotes to terrorism cannot also be applied to the other activities that might benefit the group.³ An example of this dynamic is suggested by Drake (1991, p. 54) with respect to the Provisional Irish Republican Army (PIRA) and its political wing during the group's active operations:

² With respect to nuclear terrorism, the Defense Science Board (2004, p. 28) links this point about additional resources required to gather information with attacker uncertainty, writing

If the performance of detection systems increases to the level where an attacker must conduct a complex analysis to find the chinks in our defense in order to have a reasonable expectation for success, deterrence will have reached a significant level. For example, for an attacker to have to measure background radiation around a military base exposes him to countersurveillance that he may fear, and that will increase the likelihood of successful interdiction.

³ For example, see discussion about trades between terrorism and other activities with respect to the PLO in Le Vine and Salert (1996).

One problem which could arise is a result of the greater prominence given to PSF [Provisional Sinn Féin] in the strategy of the Republican movement. If it is the case that most of the graduates and more experienced volunteers are being “creamed off” by PSF it is possible that the competence of the PIRA will be affected.

Other groups have made explicit statements about such trades. For example, Mahmud al-Zahar of Hamas was quoted as saying, “We must calculate the benefit and cost of continued armed operations. If we can fulfill our goals without violence, we will do so. Violence is a means, not a goal” (Mishal and Sela, 2006, p. 71).

Finally, efforts to seize resources from groups—through the capture of weapons, the detention of individuals, the seizure of financial assets, etc.—also affect group opportunity costs. Although such actions affect the group’s overall stocks of resources (creating internal scarcity that may simply foreclose some operational options), they also make the remaining resources relatively more valuable, and they may increase the opportunity costs of expending those resources. Captured documents from al Qaeda in Iraq illustrate the kinds of trade-offs terrorist organizations can be forced to make when resources are scarce. One document, for instance, describes a suicide mission that failed because vehicles were so scarce that one could not be spared to provide lead reconnaissance for the attack. It also describes a mission in which

the martyrs . . . were killed right before entering al Qa’im town. This was despite the man in charge of handling their transportation (Abu-al-Harith al-Salmani), [sic] knew how dangerous the road was; he requested a PKC weapon [a machine gun] for fear of clashing with the Shiites. His request was declined for lack of approval of their chief, Abu-Shahad al-Salmani, *under the pretext that weapons are scarce*. (Combating Terrorism Center at West Point, 2008, p. 9, emphasis added)

Lowering the Expected Payoff of an Operation

The expected payoff of an operation involves the terrorist’s judgment or perception of the likely utility of an operation after accounting for uncertainties about which among many possible outcomes the attack will produce. We distinguish between true expected payoffs and terrorists’ perceptions of the likely payoffs because it is terrorists’ perceptions that will drive their targeting, tactical planning, and, possibly, their decision to abandon or delay an attack (i.e., the product of successful deterrence). A planner intoxicated by the possibility of glorious success might discount the probability of failure very differently than would a more sober one, leading him or her to expect high payoffs with great certainty. It is the subjective payoff curves that will drive decisionmaking.

Similarly, we emphasize the value of the target to the terrorist rather than to the defender. Although it is reasonable to assume some rough correspondence between the utility a terrorist experiences from an attack and the disutilities to the defenders, differences in preferences, objectives, intended audiences, and other factors make for likely differences in the valuation of successful attacks both between attackers and defenders and even among different terrorist groups. Nevertheless, to the extent that terrorists design their attacks to maximize what they perceive to be defender disutilities (often considered in terms of lives lost and economic damage), reductions in defender disutilities might generally be expected to reduce the expected utility of attacks from many terrorist groups’ perspectives.

Therefore, we can consider the possibility of reducing the attacker's expected payoffs by either (1) reducing the probability of achieving any given level of payoff, thereby reducing the area under the curve describing the attacker's probability of success (e.g., p_1 in Figure 1), or (2) pushing the curve to the left, effectively reducing the expected payoff at any point on the curve. Although these are functionally equivalent, they correspond to different security approaches.

The expected payoff under the success curve is reduced when countermeasures effectively diminish the terrorist's perception of payoff for an operation. For instance, reducing the density of passengers at airline ticketing counters is intended to reduce the consequences of a suitcase-bomb attack (Stevens et al., 2004); this reduction could also reduce an attacker's perception of the expected payoff from such an attack. Similarly, payoff may be diminished by improved response and recovery capabilities. Thus, to the extent that the Strategic National Stockpile of pharmaceuticals is viewed by attackers as an effective response capability that will be brought to bear in the event of, for example, an anthrax attack, any such attack must be scored by the terrorist as likely to achieve lower casualties and economic damage than had the Strategic National Stockpile not been present.

The perceived probabilities of success, p , are shifted downward when the attacker believes security measures make the operation more difficult or risky. Hardening targets with bollards, armed guards, or security-credentialing systems may increase the attacker's sense that any given operation will be more difficult than had those security measures not been in place. With such measures in place, an attacker has two options—run the operation and accept the reduced probabilities of success or modify the operation either by raising the level of effort and resources sufficiently to overcome the security measure or by changing the target or tactic altogether (Zhuang and Bier, 2007).

Increasing Uncertainties Involved in Operation Payoffs and Costs

Many terrorist groups may be averse to engaging in operations when the likely outcomes are shrouded by significant sources of uncertainty. In addition to the empirical evidence on terrorist risk aversion discussed above, there is also evidence that, in many cases, humans generally prefer the more certain payoff when faced with an option. For instance, Kahneman and Tversky (1979) noted that, given a choice, research subjects prefer the idea of receiving a \$3,000 payment with a 100-percent chance of delivery to receiving a \$4,000 payment with an 80-percent chance of delivery, even though the expected value of the latter option is \$200 greater. Similarly, planners might be expected to prefer operations with equivalent expected payoffs but lower levels of uncertainty. Thus, returning to the example in Figure 1, even if a planner viewed the expected payoffs of Op 1 and Op 2 as roughly equivalent and the likely costs of Op 1 as substantially preferable to those of Op 2, the wide bands of uncertainty around the likely payoff from Op 1 might well tip the decision toward the more expensive Op 2.

Understanding the sources of these uncertainties for terrorist planners can aid in the design of effective security countermeasures. If attackers are sensitive to uncertainty, security interventions might be valuable even if their only effect is to increase the width of the error bar around the outcome and cost of an operation without necessarily changing the average expected payoffs or costs of the operation.

We consider three of the many general types of uncertainty that can be introduced by security systems. These sources of uncertainty figure prominently in our later discussion of our qualitative approach to measuring the relative deterrent value of security systems. Specifically, security increases uncertainty when it

- presents the attacker with defensive capabilities of unknown or unfamiliar effectiveness or operational characteristics
- pushes the attacker to adopt more-complex and more-risky tactics, such as those employing unfamiliar technologies or tactics or those with multiple failure modes
- presents the attacker with random or unpredictable security measures.

Increasing Uncertainties About Defensive Capabilities. Many game-theoretical analyses of optimal allocations of security resources assume that both the attacker and the defender have perfect information on the probability that a given operation will succeed against a specific target (see, for example, Lakdawalla and Zanjani, 2005; Bier, 2005; Golany et al., 2009). This simplifying assumption eliminates important sources of uncertainty in order to make the analysis of the “game” more tractable, but, in the case of terrorist attackers, the assumption is highly unrealistic. In truth, the likelihood of attack success is highly uncertain, depending on chance, individuals’ performance and perseverance in their duties, and security systems for which valid performance data are wholly unavailable to the attacker (and, often, the defender as well). Indeed, even after the most-careful research and reconnaissance, the attacker faces significant uncertainties about whether he or she has identified all detection and denial systems that might disrupt the planned operation, the operational characteristics of these systems, and their effectiveness.

Creating uncertainty is already a key part of some security planning. Thus, the Transportation Research Board (2002, p. 34) suggests one goal of security should be to “create a high degree of uncertainty among terrorists about their chances of defeating the system.” A similar point was made by the Defense Science Board (2004, p. 33) with respect to deterrence as part of national defense against nuclear terrorism:

The deterrent aspect of the protection equation involves the often-great differences between how a defender and an attacker will view the relative capabilities of the defense. The long history of offense/defense competitions is strongly characterized by both sides taking own-side-conservative views.⁴ More particularly, the annals of terrorism and counterterrorism are replete with instances in which a prospective attacker was deterred by aspects of the defense that may have seemed relatively weak and ineffectual to the defender. The terrorist may not be afraid to die, but he (or his master) does not want to fail. Dissuasion/deterrence by the adversary’s fear of failure might work in a variety of ways. One aspect is that an attacker will want to know enough about the defense to design a robust, successful attack. If the capabilities of the defense can be improved enough that the attacker must know the details of defensive measures in place to understand how to best surmount them, then the attacker may expose himself to discovery during the planning phases of the attack or be altogether dissuaded from the attempt. Creating uncertainty in the attacker’s mind will be critical to maximizing the success of defenses which, realistically, cannot aspire to perfection. To exploit the effects of uncertainty, the defense should be deliberately designed and deployed to create as much ambiguity for the attacker as possible as to where the “boundaries” of defense performance lie.

⁴ Although it is also the case that instances exist in which parties to potential conflicts that “should have been deterred” were not.

Uncertainties about the capabilities of counterterrorism security systems can be created through the use of partial or complete secrecy surrounding their properties or even, when deception is viable, through deceptive disclosures about their characteristics. For example, it might be advantageous for the defender to increase attacker uncertainties by broadcasting the deployment of face-recognition systems, watch lists, and informants, but obscuring the details of where these assets are deployed and how effective they are. Such issues of disclosure and deception have begun to be explored in the game-theory literature (e.g., Zhuang and Bier, 2009; Zhuang, Bier, and Alagoz, 2009; Digne, Zhuang, and Bier, 2009).

Clandestine groups are very sensitive to the risk of internal betrayal, and they often devote considerable focus to internal security (Berman, 2003). Thus, security planners might manipulate uncertainty about a terrorist organization's operational security by suggesting that the defender has collected valuable intelligence on the attacker or that the trustworthiness of the attackers' confidants (other group members, family, friends, and neighbors) is compromised. Such manipulations include deception and information operations designed to undermine the group and programs aimed at creating either disincentives for remaining loyal to the group or incentives to betray it. Examples of the second class of policies include Israel's punishment of the families of group members, particularly suicide terrorists (Almog, 2004–2005), and use of legal leverage over specific group members to force them to provide intelligence information (see Bamford, 2005). Both of these policies are ways to generate disincentives for continued group participation or loyalty. Some nations have used such efforts as amnesty programs to "extract" members from groups, thereby creating incentives to desist from terrorism (Frey and Luechinger, 2003).

Increasing Tactical Uncertainties. If all other things are equal, the probability of success becomes more uncertain as the complexity of the attack increases because additional complexity can increase the risk that something will go wrong during execution (Jackson and Frelinger, 2009a).

Such security measures as perimeter controls, armed guards, and bomb-detection systems may cause the attacker to choose to mount a more complex attack designed to neutralize the defense (with the associated cost implications discussed earlier). Doing so may require more attackers, better planning, and more-complicated or unfamiliar technology, all of which the group may or may not be able to integrate and use successfully. As complexity increases, operational security can become more difficult, training and technical-skill requirements increase, and there may be a proliferation of failure modes in the operation plan. This point was made by the Defense Science Board (2004, p. 33) in reference to security designed to counter nuclear terrorism:

A more capable and varied defense means that the attacker must mount a larger operation to penetrate it. A larger operation has more (and more observable) signatures. More people with more skills must be recruited and trained; more money must be obtained and laundered; the operation takes longer; and the attacker must surveil the defense more intensively. By increasing the signature of attack planning, the likelihood of discovery increases commensurately. This, in turn, could allow the defenses to be surged, further increasing effectiveness.

For example, for hijackers intent on gaining control of an airplane, locked and reinforced cockpit doors introduce complications that, all other things being equal, reduce the probability

of a successful hijacking operation. Tactical options are available to overcome cockpit hardening, but these may require new or unfamiliar systems—and groups may not be able to acquire or develop sufficient skill and experience in using these technologies to ensure that their actual operations are viable. An example of how security measures can increase operational complexity in more-basic ways is the protection of buildings, which requires an attacker to use multiple vehicle bombs in the attacks: An initial vehicle bomb is intended to breach the perimeter security around the building, thus allowing subsequent vehicles to closely approach their target (see, for example, an attack described by Finer and Fekeiki, 2005). Although multiple vehicle bombs are a potentially effective response to such security measures, this tactic substantially increases the complexity and risk of failure compared with a single car-bomb attack on an unprotected site.

The potential increase in attacker operational complexity resulting from physical barriers, such as perimeter security, provides a ready example for discussion. However, similar effects could result from security programs designed to provide advanced warning of attack (e.g., intelligence programs, sensor systems, behavior-detection officers), disrupt operations in progress (e.g., police- or security-officer protection of a site, locked doors, password protections), and achieve similar security aims.

Exposing Attackers to Unpredictable Security Measures. Security creates uncertainty for attackers by building in randomness and unpredictability. For example, rather than protecting a target using guard patrols that follow a defined path at regular intervals, patrols could be conducted with random frequency, timing, and routes (Pita et al., 2009). The Transportation Security Administration has several security programs designed to increase stochastic uncertainties for attackers, including the Federal Air Marshall (FAM) program, which places plainclothes armed officers on some flights, and the Visible Intermodal Prevention and Response teams, which are large groups of officers that appear, seemingly at random, at different airports over time.

If there is a 5-percent chance that a FAM or other armed law-enforcement officer will be on a plane, and if the terrorist attack's success depends on no one in the passenger cabin being armed, then, at a minimum, the attacker's assessment of the expected payoff from the operation, $E[p]$, should be diminished by 5 percent. Whether there is actually a 5-percent effect on the terrorist's subjective expected payoff will depend on how the terrorist planner responds to the possibility that the attackers will encounter the security measure. A more risk-tolerant planner might accept the additional risk to the operation and its attendant reduction in expected utility. A very conservative planner might choose to respond to the possibility by crafting a more expensive operation designed to deal with the security measure—a decision that would cause a cost-curve shift. Depending on the relative positions of the curves, this decision might result in a more significant effect.

Studies of criminal behavior suggest that a low probability of encountering a security program can have a much larger effect on decisionmaking than would be expected based on objective assessments of expected utility. For instance, Ayres and Levitt (1998) examined car thefts in communities shortly after the introduction of the LoJack system, a hidden radio transmitter used to track and recover stolen cars. They found that car-theft markets collapsed after just a small percentage of cars had installed LoJack, and stolen-vehicle rates dropped by 40 percent or more. Thus, even when the probability of encountering a security system is very low, the uncertainty created by the presence of the measure can be sufficient to lead to large-scale changes in, in this case, criminal operations.

Whether security systems with very low rates of contact with terrorists can produce significant deterrent effects is unclear. In the case of the LoJack system, the low risk of encountering a protected car might be effective because car-theft rings are exposed to it so frequently. For example, if just 3 percent of cars were protected by LoJack, professional thieves stealing 100 cars per year would have a 95-percent chance of encountering at least one LoJack device each year. Although some terrorist organizations—such as those recruiting suicide bombers for ongoing operations—could exhibit this “high-throughput” characteristic that would lead to a high probability of interaction with even a sparsely deployed security measure, it is not clear that low probabilities of detection would be equally threatening to a terrorist organization planning only a small number of operations against the United States. In the admittedly distinct case of drug traffickers, for instance, Anthony (2003, p. 5) found evidence suggesting that there appear to be thresholds in the probability of apprehension below which traffickers ignored the risk and above which the threat of apprehension successfully deterred some crime (see also Office of National Drug Control Policy, 2001). On the other hand, humans often treat low-probability aversive outcomes as far more likely than they truly are (Kahneman and Tversky, 1979), a fact which might be exploited by terrorists to drive overinvestment in U.S. counterterrorism security (Sunstein, 2003). Of course, this same tendency could also foment exaggerated concerns among terrorist planners about the likelihood that defensive measures would defeat a planned operation.

Ambiguity about the possible deterrent value of security systems with low probabilities of interdicting terrorists has led some to treat these systems as if they have no deterrent value. For instance, in their cost-benefit analysis of aviation security, Stewart and Mueller (2008) suggest that FAMs can only be effective on the flights they take, and, because they may fly on fewer than 10 percent of flights, they supply, at most, just a small protective effect. Essentially, Stewart and Mueller discount the likelihood that FAMs protect all flights through a deterrent effect regardless of whether a FAM is physically present; they do so on the grounds that FAM representation on flights is too low to serve as a meaningful deterrent, suggesting that there is a threshold at which deterrence becomes relevant and further suggesting, implicitly, that the current level of FAM deployment is below that threshold. However, Stewart and Mueller offer no justification for this claim, and they supply no method for evaluating at what point such threshold effects might be expected.

Exchanging the Relative Expected Utilities of Alternative Operations

If terrorist planners are rational and utility-maximizing, then, given a choice between two otherwise equivalent operations, one of which will produce greater utility, terrorist planners will favor the operation with the higher *net expected utility* ($E[p] - E[c]$). This assumption is not entirely safe, however, because individual groups or planners might exhibit risky decisionmaking styles that, for instance, lead them to forgo the outcome they judge to be utility maximizing in favor of a long-shot chance of achieving spectacular utilities. Nevertheless, across terrorist organizations, some strategy maximizing subjective utilities probably characterize typical decisionmaking fairly well. Therefore, if a security measure causes the net expected utility of one operation to dip below that of a second operation that also achieves the attacker's objective, the attacker is expected to prefer the second operation. Thus, the security measure will have caused risk to be displaced from the first operation to the second, a displacement that may shift the terrorism risk onto another target or cause a change in attacker operational tactics.

Because security programs may reorder terrorists' attack preferences, special consideration must be given to whether given security measures may actually increase the risk to targets valued more highly than those protected by the security system. Indeed, this insight raises an important complexity regarding risk-reduction strategies that emphasize allocating security resources to maximize per-dollar risk reduction. (See Willis et al. [2005] for a related argument.) Such a strategy may be suggested in the U.S. Office of Homeland Security's 2002 *National Strategy on Homeland Security*:

Because some activities might achieve substantial benefits at low cost, while others result in minimal gain at a high price, resources should be shifted to their most "productive" use. These shifts should be continued until the additional value of risk mitigation per dollar is equalized.

It may be easier to reduce risk to targets that the defender values less than to reduce risk to the highest-risk targets. Imagine, for instance, a city with a few iconic buildings, the locations and uses of which make them exceptionally difficult to defend. From a narrow perspective, allocating security resources to less-significant buildings might be viewed as optimizing the "productivity" of those resources, if doing so leads to large reductions in risk to the second-tier buildings. However, if the effect of these investments is that risk to the iconic buildings rises, the investments might have been unwise. Indeed, Bier (2005) has argued that there may be circumstances in which it is better to forgo further security investments if they cannot be used to reduce risk to the sites or systems valued most highly, lest improvements elsewhere increase risk where it most needs to be reduced.

The danger that risk-reduction efforts will merely lead to a displacement of risk to other targets within a class of targets is a key challenge to understanding the deterrent effects of security systems, and it will be explicitly accounted for in the approach we describe below for understanding the relative deterrent effects of alternative security systems.

Strategic, Operational, and Tactical Deterrence-by-Denial

In considering the role of deterrence in counterterrorism security planning, the critical question is how the effects of security measures on the perceived cost, utility or disutility, and uncertainties associated with particular terrorist operations can be used to shape behavior in ways that benefit the defender. Given an attack planner who views the United States and its assets and interests around the globe as a vast number of potential targets—each vulnerable to a number of attack modes with associated costs, failure risks, and payoff likelihoods—what sorts of deterrent effects might the defense attempt to produce? We briefly consider deterrence at the strategic, operational, and tactical levels as viewed from the perspective of the attacker.

Strategic Deterrence

We define *strategic deterrence* as occurring when a group is persuaded that the net expected utility of *any* attack or of a broad class of attacks is too low to permit that campaign to be favored over alternative means of pursuing the group's objectives. As such, strategic deterrence includes discouraging the use of terrorism overall as a means of achieving the group's goals, discouraging terrorist attack against the United States, or discouraging the use of an expan-

sive set of attacks, such as “all unconventional weapons options” or “all operations designed to produce mass casualties.” Earlier, we argued that the broadest type of strategic deterrence (i.e., deterrence that discourages any terrorism), may be ineffective against terrorist adversaries, particularly when pursued through deterrence-by-punishment. Others, including Quillen (2007), Roberts (2007), and Stone (2009), have argued that punishment-centered approaches may be more relevant for what Freedman (2004) refers to as a narrow strategic deterrence (e.g., deterrence that discourages the use of unconventional weapon). But could deterrence-by-denial approaches, including security measures that shape the perceived utility, costs, or uncertainties associated with terrorist operations, produce strategic deterrence?

When this question is posed with respect to many target-specific approaches to producing deterrence-by-denial, the answer is almost certainly no. The United States cannot effectively provide security for all of its interests, great and small, around the globe, so strategic deterrence is unlikely to be achieved by reducing either the probability of operational success or the payoffs associated with successful attacks. Similarly, given the differences that exist among terrorist actors, who fall along a spectrum of risk tolerance and have different requirements for the expected payoffs of attacks and other activities, ensuring that adequate protections are in place to make all operations at all targets unattractive to all terrorists sets an unrealistically high bar for protective performance—and would entail a massive resource requirement.

However, for some measures—such as broader intelligence and law-enforcement activity or border security, which provide some protection for broad classes of (or even all) targets (Powell, 2007) or specific protective measures that are very effective against specific classes of attacks—strategic deterrence may be possible for subsets of the groups that make up the overall terrorist threat to the nation. Given the vast number of groups and individuals who might consider terrorism, ranging from those who are already pursuing terrorist operations to those for whom terrorism would be a course of last resort, it is likely that credible threats of detection and apprehension might cause enough of a change in the expected utility to deter those groups wavering in indecision about how best to pursue their objectives. Measures that broadly affect the opportunity costs of terrorism, undermine the legitimacy of terrorist activity, or encourage members to leave violent groups could have similar effects at the margin.

Operational Deterrence

We define *operational deterrence* as occurring when security measures that cause shifts in the perceived utility, cost, or uncertainties associated with specific terrorist operations (or classes of operations) result in an attacker being persuaded that a particular operation should be abandoned.

An attacker who abandons one operation may simply replace it with an alternative attack. That is, security measures may deflect terrorist operations to other targets or tactics. Ideally, these new operations result in diminished disutilities to the defender, but this is not guaranteed, particularly when higher-value targets or alternative tactics that entail minimal cost or risk are available to attackers. For instance, new security measures implemented after a rash of hostage-taking attacks on U.S. embassies in the 1970s dramatically reduced the incidence of such attacks. Enders and Sandler (1993) showed, however, that attackers adapted a new and more deadly tactic: the assassination of embassy staff entering and exiting embassy grounds. In this case, increasing the failure risk for the original mode of attack may have encouraged a shift to an attack strategy that was more lethal and unfavorable to U.S. interests.

Used deliberately, operational deterrence attempts to manipulate terrorist choices to produce net security benefits. It may be the form of deterrence over which security planners have the greatest control, insofar as countermeasures designed to improve detection, denial, and target resiliency should directly affect terrorist planners' calculations of the net expected utility of individual operations. Used carefully, security countermeasures could shift operations to targets with lower expected payoffs for attackers (which are damages, from the defender's perspective) either because they force the attacker to adopt riskier tactics and technologies, thereby reducing the attackers' true probability of success (as opposed to the attacker's perception of success probability), or because they increase the attacker's costs sufficiently to delay or deter the attack.

For security planners, *using* operational deterrence requires attempting to anticipate the changes that terrorist organizations might make when new security measures are put in place. Whether operational deterrence can be used to produce security benefits requires knowing what the next most attractive target or attack mode might be. For example, in addressing the threat of suicide bombers in Israel, enclosed shopping malls deployed armed guards to deny access to bombers. This greatly reduced attacks within the malls, but terrorists instead began launching attacks at the mall entrances and in open air malls and restaurants, which are more difficult to defend. However, there was a deterrence benefit, since the measure moved the explosion from "a closed area where the impact of the blast would have been very powerful, [to a more open one] where the impact was weaker" (Perliger and Pedahzur, 2006, p. 283). Israel's adoption of a security barrier in the West Bank to limit the infiltration of suicide bombers into the country had a similar, but broader, effect. In that case, the operational deterrence that occurred was greater use of rockets to stage stand-off attacks into the country, an attack mode that had a much smaller probability of success and produced many fewer casualties. Because that attack mode is inferior to suicide bombers, the security benefit is positive (case-study examples are found in Jackson et al., 2007).

Whether a security measure is viewed as a credible barrier to success also depends on the beliefs, capabilities, motivations, and experience of the attacker. The deterrent effects of a given security measure will therefore be attacker specific. As noted by Le Vine and Salert (1996, p. 23),

a leader who has to decide whether to send people to engage in terrorism is likely to base his or her decision on the likely consequences to that group, rather than to all groups. A PLO leader with well-trained personnel might not have been overly impressed by the fact that some "amateur" group was quickly apprehended in some country—he might have reasonably inferred that that was due to their ineptitude.

Finally, the value of operational deterrence can also depend strongly on the point of view of the security decisionmaker. To a security planner responsible for a single target, shifting an attack to a target next door is a success, albeit a parochial one. To a higher-level security planner, whether there is a net security gain from such deterrence depends on the relative disutilities of the two targets.

Tactical Deterrence

We have focused on terrorist perceptions of the utility, costs, and uncertainties surrounding particular operations during the planning phase of an attack that occurs before the execution

of the operation. Terrorist estimates of these parameters could change even after an operation is initiated—but before it reaches completion—which may also create an opportunity for what we call *tactical deterrence*. As an operation progresses (for example, as attackers are en route to the target), the terrorists may continue to receive new information that could cause them to reevaluate the attack. To the extent that their activities are still clandestine, it is possible for attackers to call off an in-progress operation if they are persuaded that the probability of operational success (or its likely net payoff) has declined to unacceptable levels. It is also possible that they will take adaptive action to try to raise that probability again.

When security organizations have extensive information about terrorist plots, organizations, and activities, tactical deterrence can be used in a very deliberate and surgical way. For example, in Northern Ireland, British security forces operating against PIRA had gained extensive intelligence about the group through a variety of means, including human sources within the group. Although some of that information could not be used as the basis for arrest or prosecution of the individuals involved, intelligence and law-enforcement organizations were able to use it to cause PIRA to halt its attacks. For example, Urban (1992, p. 213) quotes a British intelligence officer who described

one incident where it was known that a [PIRA] team was to travel along a particular route on its way to an attack. They [the security forces] arranged for a car “accident” to take place on the road. “There wasn’t a uniform in sight,” he recalls, “but it was assumed that they [the insurgents] would get unnerved sitting in the tailback, thinking the police were about to arrive.” The ploy succeeded.

Veness, a British counterterrorism official, generalizes that “deterrence can be achieved by overt activity intended to counter the terrorist at the reconnaissance, preparation, attack, and escape phases” (Veness, 1999, p. 14).

Both increasing security in response to threats and making frequent, unpredictable changes in security procedures may create tactical deterrent effects as attackers discover upon arrival that security measures at their intended target are not what they expected. Such changes might result in a halt or adjustment to the attack. Schmitt and Shanker (2006) provide an example:

[I]n 2002, Iyman Faris, a naturalized American citizen from Kashmir, began casing the Brooklyn Bridge to plan an attack and communicated with Qaeda leaders in Pakistan via coded messages about using a blowtorch to sever the suspension cables. But by early 2003, Mr. Faris sent a message to his confederates saying that “the weather is too hot.” American officials said that meant Mr. Faris feared that the plot was unlikely to succeed—apparently because of increased security.

Hoffman (2003) cites an Israeli case in which tactical deterrence resulted merely in the modification of an attack plan:

[A] female suicide bomber tried to enter the Mahane Yehuda open-air market—the fourth woman to make such an attempt in four months—but was deterred by a strong police presence. Instead, she walked up to a bus stop packed with shoppers hurrying home before the Sabbath and detonated her explosives, killing six and wounding seventy-three.

Similar uncertainties can be created in attackers' minds by releasing information (e.g., public warnings that intelligence has identified indicators of attacks on a particular sector or set of targets) that causes attackers to question what else might be known about their plans.

Analyzing the Deterrent Effects of Security Measures

Our discussion demonstrates that security systems cannot be characterized as having an *inherent* level of overall deterrent effect. Instead, since even successful operational and tactical deterrence can lead to risk displacement, the deterrent effects of any component of the national homeland security architecture depend to a great degree on the characteristics of the *entire* security architecture. For example,

- A security program that effectively discourages shipment of nuclear materials through major ports might still be a weak deterrent of nuclear attack if attackers can just as easily import such materials via smaller ports, land crossings, or other gaps in the security architecture.
- Effective risk reduction for a single nuclear power plant may achieve little overall deterrence against an attack on the nuclear power infrastructure of the United States.
- The operational deterrence produced by a security system that denies one type of attack but permits another equally destructive attack that is no more difficult to mount is unlikely to produce a net security benefit. In fact, it may even lead to attacks that are more damaging to U.S. interests than the attack that was prevented.

Conversely, if multiple components of the national homeland security architecture work effectively together so that attackers deterred from attacking one entry point, particular target, or tactical option have no good alternatives, a measure that might look like a weak deterrent on its own could have substantial, even strategic, deterrent value.

Because of this deep dependence on the broader homeland security architecture, a claim that a specific individual security program or its features serve as a deterrent against specific attacks requires an explicit demonstration that simple workarounds are also denied by some other part of the nation's security system. Moreover, because different targets and attack modes may be substituted for those denied by a security program, deterrence must also be understood to range from a narrow operational deterrence (that might protect an individual person or place) to progressively more-strategic forms of deterrence (that might deny most plausible attacks against an entire class of objects, such as airplanes or airports) to broad strategic deterrence (that might afford protection to the country as a whole or to entire sectors of strategically important assets). Assessing the deterrent value of any given security measure therefore requires adopting a systems perspective, in which the value of the measure is weighed in the context of the overall homeland and national security system of which it is a part.

Finally, analysis of deterrent effects also depends to a great extent on understanding the unique evolving preferences, beliefs, and capabilities of specific individuals and groups that are considering a terrorist attack against the United States. Some groups will be more readily deterrable than others.

Together, these characteristics highlight that understanding the deterrent effect of systems requires in-depth analysis of the options available to specific attackers with specific intentions,

capabilities, and beliefs. Such analysis requires carefully working through multiple attack strategies, reverse-engineering them to explore requirements critical to their success and estimating the costs and capabilities required to employ alternative strategies. The difficulty in making precise or accurate measures of these variables makes clear the challenge of attempting to make absolute statements about the deterrent effects of security systems.

A detailed analysis of the national homeland security architecture goes well beyond the scope of this paper. Instead, we consider how such an analysis could be directed to assemble information on the critical components of deterrence just described, allowing a *qualitative* assessment of the relative deterrent value of individual security programs to be produced.

Specifically, we suggest a framework for resolving the likely deterrent effects of a system into a small number of factors that appear most likely to increase terrorists' perceptions of the expected operational costs, reduce their perceived expected payoffs, and increase their uncertainty about particular activities or attacks on specific targets. To illustrate our approach, we make crude judgments about whether these costs and payoff risks are low, medium, or high; careful analysis or good intelligence could be used to improve the resolution of the analysis. Similarly, because both costs and payoffs depend significantly on the characteristics of individual terrorist organizations, the analysis should consider the specific attackers the security measure is designed to counter rather than taking the approach we adopt here, which is to arrive at general statements about typical expected costs and payoff risks. Nevertheless, we believe the framework we supply offers some hope of improving the systematicity of analysis, or at least of making explicit the otherwise implicit judgments that inform claims about the deterrent value of counterterror systems.

Two main cost drivers shape the decision to mount an operation despite the presence of a security system or multiple, layered systems. Because terrorists can substitute a softer target or make additional investments to defeat or evade the security measure, we have labeled the first of these drivers the *cost to evade/defeat* the security measures. The second cost driver, the *cost of engagement* with the security measure, concerns the likely risks to the operation of engaging the security system if measures are not taken to evade or defeat it, both in terms of reduced operational payoffs and direct costs to the organization (such as loss of personnel). These two costs reflect the hardships that the security system imposes on the terrorist group, whether it voluntarily pays the cost to evade/defeat the measure or the cost is imposed on the attackers when they engage the security measure without investing in a workaround.

The cost to evade/defeat might involve increasing force levels without modifying the attack mode, or it might involve changing the attack mode to avoid or defeat the security system. For instance, operations threatened by the possible presence of a FAM, chiefly those designed to gain control of an airplane, must either overpower the FAM or avoid engaging him or her. Because options for overcoming or avoiding the FAM present significant logistical challenges, the cost to evade/defeat a FAM might be rated as high or medium, depending on an attacker's capabilities. In general, the more "expensive" a security measure is for groups to overcome, the greater its potential deterrent value. In contrast, as noted in the recent National Research Council (2009) review of the Advanced Spectroscopic Portal program, if inexpensive alternatives for simply avoiding or working around the security system exist, the system is unlikely to exert any meaningful deterrent effect.

For purposes of illustration, we assign a *low* cost to evade/defeat to security programs when changes to the attacker's operation that are well within the organization's capabilities are likely to result in successfully defeating or avoiding the system. A *medium* cost to evade/

defeat is assigned to security systems when workarounds to avoid or defeat the system entail considerable risks or costs that may be difficult for the attacker to bear. A *high* cost to evade/defeat is assigned to systems that present the attacker little chance of either avoiding or defeating the system because all plausible defeat and avoidance strategies entail risks or costs deemed unacceptably high.

Even a security system that cannot be successfully defeated or avoided will not necessarily achieve a deterrent effect. Its likelihood of creating a deterrent effect depends on how “expensive”—in terms of real costs or added risk—it will be for the attackers when they encounter it. If the cost of engaging the security measure is minimal, the measure cannot be expected to exert a significant deterrent effect. For instance, if the likely price of a failed cyber attack is that the attacker loses control of a few hijacked computers he or she had successfully exploited in another country, this might not represent a significant loss for most groups. If the price of failure is the loss of a suicide bomber without achieving the intended payoff, this could be a significant concern for a group with limited suicide-bomber resources, whereas, for a group rich in such personnel, the cost might be modest. Returning to the FAM example, if the price of failure was both the loss of a several key group members and waste of an operation that took months or years to plan and implement, this might be a moderate to high cost for most groups.

For the cost of engagement, therefore, we propose that low values correspond to security systems that present attackers with modest costs, modest risks of failure, and modest expected consequences for the attacker who must engage with the security system. Medium values go to systems that present attackers with costs or consequences that are likely to be viewed as presenting a significant hardship to the organization or that present a risk of operational failure that the attacker views as nontrivial. High values correspond to systems likely to produce unacceptably high costs, consequences, or risks of failure.

The final component of the deterrence calculation concerns the likelihood that security measures will effectively engage the attack. This probability is a function of many factors, chief among which are the probability of *encountering* such a security system and the probability that the system will *detect* the operation as a threat and successfully impose the cost of engagement just discussed. For instance, Stewart and Mueller (2008) suggest that FAMs are present on fewer than 10 percent of U.S. flights, so, suppose the probability of encountering one on any flight is approximately 0.05. If they are on a flight, the chance that they can both detect and impose their costs of engagement on the attacker seems reasonably good, so, for the sake of argument, we assume that the presence of a FAM on a flight will make the probability of detection and successful engagement 1.0. This suggests that the per-operation likelihood that security operations will effectively engage the attackers is 0.05 ($0.05 * 1 =$ the probability of encountering a FAM $* \text{probability of a FAM detecting and successfully engaging the threat}$). A 5-percent risk may be too high for groups with limited capabilities. If the group had only one hijack team and all its plans hinged on the attack being successful, a 1 in 20 chance of failure might not be acceptable. However, if the terrorist group could mount three such operations simultaneously, and if it only required one of those attacks to succeed to achieve its goals, the probability that FAMs would effectively deny the overall attack (comprising its redundant pieces) plunges to about one in 1,000, a risk of failure that many groups might judge acceptable.

For the likelihood of engagement with the security system, scores of low, medium, or high would be assigned based on the analyst’s judgment of the level of risk tolerance exhibited by the terrorist organization. These levels would range from those likely to be discounted as

negligible by the group to those likely to be viewed as moderate to those likely to be viewed as presenting a near certainty that security measures would effectively engage the attackers.

Figure 2 offers a notional system for scoring the deterrent effects of security systems based on the cost to evade/defeat, the cost of engagement, and the likelihood of effective engagement. Deterrence is scored on a scale from 0 (no meaningful deterrence) to 5 (the highest level of deterrence). In this construct, counterterror systems that are not particularly hard to overcome or that pose minimal costs to terrorists are presumed to have no meaningful deterrent effect no matter how likely it may be that attackers will have to engage such systems. The highest deterrence effects are expected from systems that would be unacceptably hard to thwart, whose cost of engagement would be unacceptably high, and that are especially effective in detecting and imposing the costs of engagement on the threats they are designed to interdict. Between these extremes, we offer a range of judgments about the relative deterrent effects of systems with different characteristics.

Data on some criminal organizations and terrorist activities support the idea that it is the *combination* of these types of factors that produces deterrence. In a close examination of Peruvian cocaine trafficking, Anthony (2004, p. 49) showed that

with the threat of lethal force [a high cost of engagement], an 8 to 10 per cent interception rate [a modest probability of successful engagement] held down trafficking to less than 15 per cent of former levels, causing the collapse of the Peruvian cocaine trade. Less severe consequences [lower costs of engagement] worked at higher interception rates [higher probabilities of successful engagement] in the transit zone to the United States.

Analyses of skyjackings have similarly examined both measures (the likelihood and costs of engagement) in seeking to identify deterrent effects on different terrorist and nonterrorist actors (Chauncey, 1975; Dugan, LaFree, and Piquero, 2005).

The scheme presented above is designed exclusively for calculating the likelihood that a counterterrorism security measure will deter attacks against the specific target, site, or system directly protected by the security measure. This kind of narrow operational deterrence does not ensure that attacks will not merely be shifted to sites that are less protected.

Figure 2
Candidate Deterrence-Level Analyzer

Cost to evade/defeat	Cost of engagement	Likelihood security measures effectively engage attack		
		Low	Medium	High
High	High	3	4	5
High	Medium	2	3	4
Medium	High	2	3	4
Medium	Medium	1	2	3
Low	(Any)	0	0	0
(Any)	Low	0	0	0

When considering more-strategic protection of a broad class of targets, or when examining defense from a regional or national perspective, another dimension of deterrence must be evaluated. For example, if attacks against a particular building are deterred by improved building-security procedures but the building is part of a class of comparable terrorist targets that have not received similar security improvements, *from the standpoint of the class of targets*, the system may have no deterrent effect. That is, if the security measure merely deters attacks by shifting them to other members of a class of targets, the system has no net deterrent value viewed from the perspective of the class, which might be a city (which could contain several such targets), a state (which could contain many such targets), or the country overall (which contains the entirety of the class).

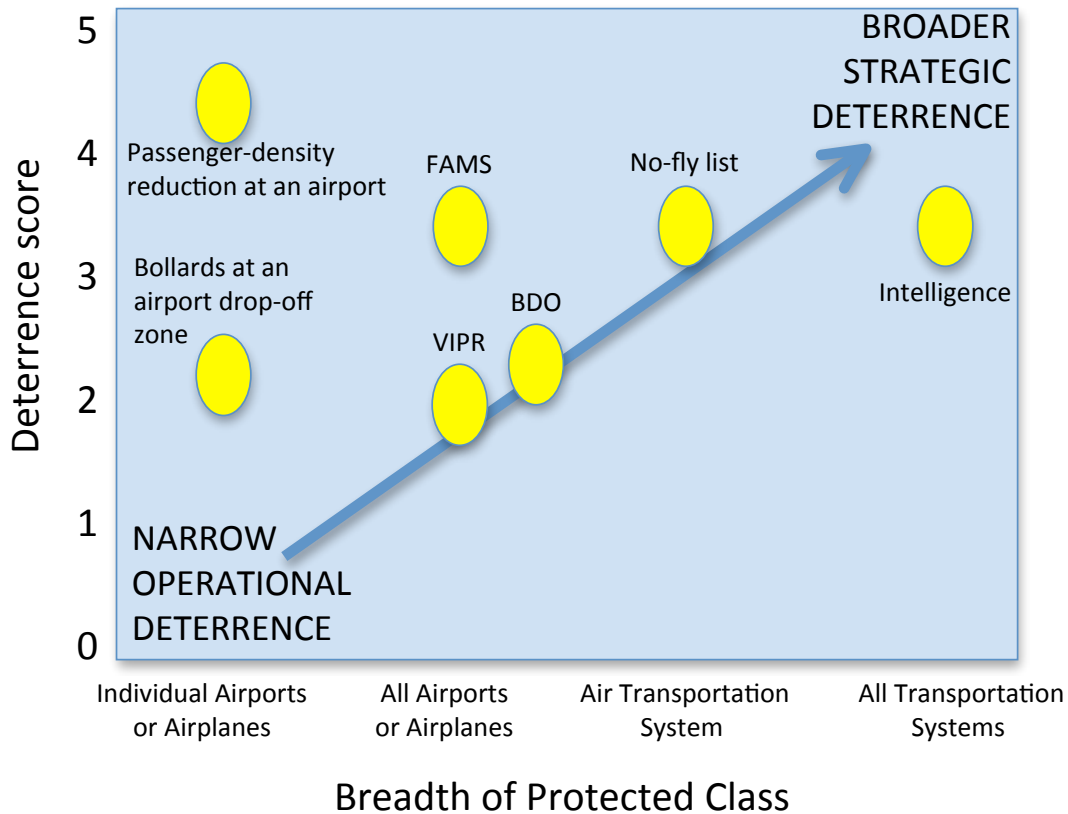
Although the building manager or some analogous security manager with a limited scope of responsibility within a broader class of targets might rate the deterrent value of a security measure using the table presented in Figure 2, executive security managers, such as those responsible for administering federal homeland security grant funding must also consider the breadth of the class of potential targets a system is likely to protect through deterrence. In some cases, the class in question might be quite narrow. For instance, there may be a small number of federal buildings deemed sufficiently important (and sufficiently attractive to attackers) that deflection of attacks on these buildings to buildings of lesser importance represents a key objective of security. In other cases, the class might be conceptualized as very large (for example, all transportation systems in the United States). This consideration requires us to lay our one-dimensional deterrence score for a security measure along a second dimension that considers the breadth of protection offered by the system. That is, the greatest deterrence benefits (i.e., the most-strategic deterrence) is expected from systems that protect the widest class of targets and offer the greatest level of deterrence.

Figure 3 illustrates the type of result that might be produced through such an analysis for the class of all air transportation systems. We offer this figure for illustrative purposes, and emphasize that we have not undertaken the kinds of analysis that would be required to correctly assess the values of the security measures depicted here. In this figure, the relative deterrent value from the perspective of general transportation security of seven representative counterterrorism security measures are compared. At the lower left of the figure are programs that offer only narrowly operational deterrence, which provides weak deterrent value for the class. To the upper right would be those programs offering stronger more strategic deterrence across the entire class of targets.

A possible implication of this analysis is that, as classes become more broad and national in scope, it is the security strategies that are the most general that will have the greatest collective deterrent value, not the strategies that defend specific targets against specific threats. For instance, intelligence, no-fly lists, and other detection systems may result in the prevention of a far broader range of operations than measures undertaken to defend individual points of vulnerability (Powell, 2007).

In addition to offering protection to a wide range of targets, intelligence programs have the effect of suppressing the entire probability-of-success curve described in Figure 1. Whereas improved security offered by FAMs may cause the probability of success to taper for a narrow set of operations, the risk of detection and disruption posed by an effective intelligence program affects the success of the same operations—and many others—that target other transportation modes, thereby requiring attackers to choose other modes of attack or other ways of adapting. Moreover, to the extent that the detection and surveillance capabilities of the

Figure 3
Notional Classification of the Relative Deterrent Value of Various Air-Transportation Counterterrorism Security Systems



NOTE: FAMS is the Federal Air Marshall Service, VIPR is the Visible Intermodal Prevention and Response program, and BDO is the Behavior Detection Officer program.

intelligence program are unknown to the terrorist, the possible existence of such programs may cast a heavy cloud of uncertainty over the success probability, with discouraging results for operational planners.

Discussion

Understanding whether a counterterrorism security system serves as a deterrent—and how well it deters attacks—is vitally important to security planning. Indeed, in some cases, the returns expected from investments in major federal security programs may depend largely on these deterrent effects. Nevertheless, no satisfactory methods exist to measure the deterrent value of such programs. Indeed, in some texts on the actual design of security systems, deterrence is viewed as so abstract and unquantifiable that it should not be considered in design and instead should simply be seen as an “extra benefit” produced by a well-implemented security system (see, for example, Garcia, 2001).

In the absence of systematic measurements, legislators and senior executives must rely on their own or others' intuitions about likely deterrent effects, and these judgments may be difficult to justify or apply consistently across diverse security programs. Moreover, because deterrence has not been well defined, there is a risk that, without an explicit conceptual model describing what is meant by *deterrence*, the concept of deterrence may be used inconsistently by different people or programs. Whereas a hotel manager might be referring to very narrow operational deterrence (and might be satisfied with deflecting possible attacks to the hotel down the street), a federal policymaker may be emphasizing a form of operational deterrence that is so broad that it amounts to strategic deterrence.

This paper attempts to develop an analytic framework for understanding the deterrent effects of security systems by resolving these effects into component judgments that terrorists can be expected to make about how the security program affects their perceived costs, benefits, and uncertainties and the alternative operations available to them in pursuit of their objectives. In doing so, we highlight important distinctions that must be made about the types of deterrence that security programs might be expected to achieve (tactical, operational, or strategic deterrence) and emphasize that the inescapable fact of risk displacement forces any judgment of the deterrent effects of a given security program to be premised on a high-level systems understanding of the national homeland security architecture.

Because deterrent effects are contingent on subjective and idiosyncratic terrorist organizational planning, the measurement of security-system deterrent effects is necessarily imperfect. Nevertheless, by resolving the components of a deterrent effect into constituent factors, each to be judged qualitatively, the method offers a means for clarifying and making explicit the assumptions that go into potentially conflicting judgments about a system's value as a deterrent.

Many security decisionmakers want to know the specific level of strength or reliability of security systems that is necessary to achieve deterrence. For instance, many people share the intuition that a system with 100-percent reliability for detecting the presence of radiological materials in shipping cargo containers may be overkill. Surely, a terrorist organization would not risk sending such potentially valuable weapons through a system with 99-percent reliability, or even one with 80-percent reliability. Indeed, the behavior of smugglers of less-dangerous cargo suggests that deterrence thresholds do exist and that they could be significantly below 50 percent *if* the perceived cost of engaging the security measures is high (Anthony, 2003), which the loss of a nuclear device would almost certainly be for a terrorist group attempting to smuggle such a device into the United States.

This paper's framework for analyzing deterrent effects highlights some of the complexities that must be addressed before such threshold effects can be established. In the case of radiological materials, for example, many pieces of information are crucial: a comprehensive assessment of what alternative infiltration strategies the national radiological defense architecture offers, estimates of how expensive and risky it would be to attempt to defeat the port-security system, and estimates of terrorists' capabilities, resources, and risk tolerance, among other factors. With this information, rough judgments about the system reliability thresholds required to deter a particular terrorist group could be produced by estimating the expected utility to the terrorists, from their perspective, of bringing radiological materials into the country through the ports rather than through the next-most promising route. Whatever level of reliability of the port-screening system would cause the terrorists to judge that infiltration method to be no better than the next-best method would be, in principle, the threshold above which the cargo-security system could be expected to exert a deterrent effect. However, this effect would be

only a narrowly operational deterrent that displaces the infiltration attempt to the next-most promising route.

Unfortunately, the information required for this type of analysis will never be known with precision by the defender, so any threshold estimate will necessarily be subject to wide error bands. Nevertheless, the cost of trying to implement systems with near-perfect reliability may be prohibitive, in which case even imperfect estimates of deterrence threshold effects may be a valuable aide for resource-allocation decisions.

Whereas an analysis of deterrence threshold effects like that described above would require an intensive and probably time-consuming effort, we believe that the framework we present here could be of immediate use to decisionmakers faced with making resource-allocation decisions based only on their own expert judgments and those of subject-matter experts. Specifically, by breaking these expert judgments down into component judgments about alternative systems (specifically, the relative cost to evade/defeat, the cost to engage, the likelihood of engaging, and the breadth of coverage each system offers), the judgments of multiple experts can be systematically compared and integrated into a uniform, conceptually standardized assessment of the relative deterrent value of the multiple systems—information that may be useful in making resource-allocation decisions.

Moreover, the analyses we develop here make several points about deterrence that are important for security managers to consider, including the following:

- While some have argued that deterrence is largely irrelevant for terrorists—and suicide terrorists in particular—it is clear that some types of deterrence are indeed quite relevant to the contemporary terrorist threat. In this paper, we have explored how the deterrence-by-denial produced by implementing security measures at individual targets or more broadly can operate at the tactical and operational levels. In some cases, the net effect of such deterrence could produce strategic deterrence for classes of targets or types of attacks. Moreover, deterrence-by-punishment approaches may indirectly affect terrorist capabilities, if they influence the behavior of the actors that attack planners interact with or depend on (Davis and Jenkins, 2002; Freedman, 2004), although deterrence-by-punishment was not the primary focus of this discussion.
- Operational-level deterrence and the resulting risk displacement are important phenomena that may have major effects on security and on the cost-effectiveness of security systems. When not assessed during the process of designing security strategies, the displacement of risk that operational or tactical deterrence can produce is a significant threat to the value of security investments. But if such effects are built into security plans, they could assist in magnifying rather than diluting protective effects.

The potential for risk displacement makes understanding the deterrent effect of a security program a systems problem. Whether baggage screening produces a strong, broad deterrence against attacks on airplanes depends critically on the effectiveness of the entire national transportation-security architecture. If attackers have few other good options for getting weapons onto planes, the risk that baggage screening will disrupt a planned attack might deter terrorists from attacking air-transportation targets. If alternatives are readily available, however, there may be no deterrence from attacks on aviation. Without carefully working through the options available to terrorist planners, security programs may not only fail to deter attacks: They may even lead to unintended negative outcomes, such as occurred when the lethality of embassy attacks increased after barri-

cade and hostage attack methods were made more difficult by security measures (Enders and Sandler, 1993).

- Counterterror security planners probably have greatest influence over operational deterrence because they can increase the perceived costs or decrease perceived payoffs of an attack and because they can increase uncertainty associated with attack benefits and risks. Representing the components of a terrorist's decision calculus as exceedance curves, as we have done in this paper, emphasizes the role that uncertainty plays in such decisions even in the absence of security countermeasures. It also emphasizes the potential for defensive efforts to magnify those uncertainties.

Whereas operational deterrence falls short of the goal of preventing future attacks against the United States, it can be used strategically to shift attacks to less-damaging methods or targets. Using operational deterrence to shift terrorist planners away from attacks with nuclear weapons, for example, could represent an important strategic accomplishment.

- Deterrent effects depend on the characteristics of the groups considering an attack—specifically, their preferences, beliefs, capabilities, and levels of risk tolerance. Although it might be possible to manipulate each of these factors through careful security planning and operations, variations across terrorist groups suggest that deterrence should be evaluated, when possible, in light of what is known about the individual groups against whom a security system is chiefly designed.

Bibliography

- Almog, D. (2004–2005). “Cumulative Deterrence and the War on Terrorism,” *Parameters*, Winter 2004–2005, pp. 4–19.
- Anthony, R. (2004). “A Calibrated Model of the Psychology of Deterrence,” *Bulletin on Narcotics*, Vol. LVI, Nos. 1 and 2, pp. 49–64.
- Anthony, R. W. (2003). *Deterrence and the 9-11 Terrorists*, Institute for Defense Analyses, D-2802.
- Ayres, I., Levitt, S. (1998). “Measuring Positive Externalities from Unobservable Victim Precaution: An Empirical Analysis of Lojack,” *Quarterly Journal of Economics*, Vol. 113, No. 1, pp. 43–77.
- Bamford, B. W. C. (2005). “The Role and Effectiveness of Intelligence in Northern Ireland,” *Intelligence and National Security*, Vol. 20, No. 4, pp. 581–607.
- Becker, G. (1968). “Crime and Punishment: An Economic Approach,” *The Journal of Political Economy*, Vol. 76, pp. 169–217.
- Berman, E. (2003). “HAMAS, Taliban, and the Jewish Underground: An Economist’s View of Radical Religious Militias,” NBER Working Paper No. 10,004.
- Bier, V. (2005). *Choosing What to Protect*, CREATE Report 05-001, University of Southern California.
- Bowen, W. Q. (2004). “Deterrence and Asymmetry: Non-State Actors and Mass Casualty Terrorism,” *Contemporary Security Policy*, Vol. 25, pp. 54–70.
- Boyne, S. (2006). *Gunrunners: The Covert Arms Trail to Ireland*, Dublin: O’Brien Press.
- Caulkins, J. P. (1993). “Local Drug Markets’ Response to Focused Police Enforcement,” *Operations Research*, Vol. 41, No. 5, pp. 848–863.
- Chauncey, R. (1975). “Deterrence: Certainty, Severity, and Skyjacking,” *Criminology*, Vol. 12, No. 4, 1975, pp. 447–473.
- Combating Terrorism Center at West Point (2008). “Analysis of the State of ISI,” NMEC-2007-612449.
- Cook, P. J. (1980). “Research in Criminal Deterrence: Laying the Groundwork for the Second Decade,” *Crime and Justice*, Vol. 2, pp. 211–268.
- Davis, P., Jenkins, B. M. (2002). *Deterrence and Influence in Counterterrorism: A Component in the War on al Qaeda*, Santa Monica, Calif.: RAND Corporation, MR-1619-DARPA. As of November 3, 2009: http://www.rand.org/pubs/monograph_reports/MR1619/
- Defense Science Board (2004). *Report of the Defense Science Board Task Force on Preventing and Defending Against Clandestine Nuclear Attacks*, Washington D.C.: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics.
- Digne, N. S., Zhuang, J., Bier, V. (2009). “Secrecy in Defensive Allocations as a Strategy for Achieving More Cost-Effective Attacker Deterrence,” *International Journal of Performance Engineering*, Vol. 5, No. 1, pp. 31–43.
- Drake, C. J. M. (1991). “The Provisional IRA: A Case Study,” *Terrorism and Political Violence*, Vol. 3, No. 2, pp. 43–60.
- Dugan, L., LaFree, G., Piquero, A. R. (2005). “Testing a Rational Choice Model of Airline Hijackings,” *Criminology*, Vol. 43, No. 4, pp. 1031–1065.

- Dutter, L. E., Seliktar, O. (2007). "To Martyr or Not to Martyr: Jihad Is the Question, What Policy Is the Answer?" *Studies in Conflict and Terrorism*, Vol. 30, No. 5, pp. 429–443.
- Enders, W., Sandler, T. (1993). "The Effectiveness of Anti-Terrorism Policies: Vector Autoregression Intervention Analysis," *American Political Science Review*, Vol. 87, pp. 829–844.
- Enders, W., Sandler, T. (2002). "Patterns of Transnational Terrorism, 1970–1999: Alternative Time Series Estimates," *International Studies Quarterly*, Vol. 46, pp. 145–165.
- Finer, J., Fekeiki, O. (2005). "Assault on Hotel Kills 16 in Baghdad," *The Washington Post*, October 25, 2005.
- Freedman, L. (2004). *Deterrence*. Malden, Mass.: Polity Press.
- Frey, B. S., Luechinger, S. (2003). "How to Fight Terrorism: Alternatives to Deterrence," *Defence Peace Economics*, Vol. 14, pp. 237–249.
- Frey, B. S., Luechinger, S. (2004). "Decentralization as a Disincentive for Terror," *European Journal of Political Economy*, Vol. 20, pp. 509–515.
- Garcia, M. L. (2001). *The Design and Evaluation of Physical Protection Systems*, Boston.: Butterworth Heinemann.
- Golany, B., Kaplan, E. H., Marmur, A., Rothblum, U. G. (2009). "Nature Plays with Dice—Terrorists Do Not: Allocating Resources to Counter Strategic vs. Probabilistic Threats," *European Journal of Operations Research*, Vol. 192, pp. 198–208.
- Helfstein, S., et al., (2009). "White Paper Prepared for the Secretary of Defense Task Force on DoD Nuclear Weapons Management: Tradeoffs and Paradoxes: Terrorism, Deterrence and Nuclear Weapons," *Studies in Conflict & Terrorism*, Vol. 32, No. 9, pp. 776–801.
- Hoffman, B. (1997). "The Modern Terrorist Mindset: Tactics, Targets and Technologies," Center for the Study of Terrorism and Political Violence, St. Andrews University. As of April 22, 2009: <http://www.ciaonet.org/wps/hob03/>
- Hoffman, B. (2003). "The Logic of Suicide Terrorism," *Atlantic Monthly*, June 2003.
- Hope, B. (2006). "Price of Illegal Guns Soaring Here in Wake of Anti-Gun Campaign," *The Baltimore Sun*, November 1, 2006.
- Jackson, B. A. (2009a). *Marrying Prevention and Resiliency: Balancing Approaches to an Uncertain Terrorist Threat*, Santa Monica, Calif.: RAND Corporation, OP-236-RC. As of November 3, 2009: http://www.rand.org/pubs/occasional_papers/OP236/
- Jackson, B. A. (2009b). "Organizational Decisionmaking by Terrorist Groups," in P. K. Davis and K. Cragin, eds., *Social Science for Counterterrorism: Putting the Pieces Together*, Santa Monica, Calif.: RAND Corporation, MG-849-OSD. As of November 3, 2009: <http://www.rand.org/pubs/monographs/MG849/>
- Jackson, B. A., (2009c). *The Problem of Measuring Emergency Preparedness: The Need for Assessing 'Response Reliability' as Part of Homeland Security Planning*, Santa Monica, Calif.: RAND Corporation, OP-234-RC. As of November 3, 2009: http://www.rand.org/pubs/occasional_papers/OP234/
- Jackson, B. A., Chalk, P., Cragin, R. K., Newsome, B., Parachini, J. V., Rosenau, W., Simpson, E. M., Sisson, M., Temple, D. (2007). *Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies*, Santa Monica, Calif.: RAND Corporation, MG-481-DHS. As of November 3, 2009: <http://www.rand.org/pubs/monographs/MG481/>
- Jackson, B. A., Frelinger, D. R. (2009a). *Emerging Threats and Security Planning: How Should We Decide What Hypothetical Threats to Worry About?* Santa Monica, Calif.: RAND Corporation, OP-256-RC. As of November 3, 2009: http://www.rand.org/pubs/occasional_papers/OP256/
- Jackson, B. A., Frelinger, D. R. (2009b). *Understanding Why Terrorist Operations Succeed or Fail*, Santa Monica, Calif.: RAND Corporation, OP-257-RC. As of November 3, 2009: http://www.rand.org/pubs/occasional_papers/OP257/

- Kahneman, D., Tversky, A. (1979). "Prospect Theory: An Analysis of Decision Under Risk," *Econometrica*, Vol. XLVII, pp. 263–291.
- Keohane, N. A., Zeckhauser, R. J. (2003). "The Ecology of Terror Defense," *Journal of Risk and Uncertainty*, Vol. 25, pp. 201–229.
- Kleck, G., Sever, B., Li, S., Gertz, M. (2005). "The Missing Link in General Deterrence Research," *Criminology*, Vol. 43, No. 3, pp. 623–659.
- Lakdawalla, D., Zanjani, G. (2005). "Insurance, Self Protection and the Economics of Terrorism," *Journal of Public Economics*, Vol. 89, pp. 1891–1905.
- LaTourrette, T., Howell, D. R., Mosher, D. E., MacDonald, J. (2006). *Reducing Terrorism Risk at Shopping Centers: An Analysis of Potential Security Options*, Santa Monica, Calif.: RAND Corporation, TR-401. As of November 3, 2009:
http://www.rand.org/pubs/technical_reports/TR401/
- Le Vine, V. T., Salert, B. A. (1996). "Does a Coercive Official Response Deter Terrorism? The Case of the PLO," *Terrorism and Political Violence*, Vol. 8, pp. 22–49.
- Long, A. (2008). *Deterrence—From Cold War to Long War: Lessons from Six Decades of RAND Research*, Santa Monica, Calif.: RAND Corporation, MG-636-OSD/AF. As of November 3, 2009:
<http://www.rand.org/pubs/monographs/MG636/>
- Major, J. A. (2002). "Advanced Techniques in Modeling Terrorism Risk," *Journal of Risk Finance*, Fall 2002.
- Mishal, S., Sela, A. (2006). *The Palestinian Hamas: Vision, Violence, and Coexistence*, New York: Columbia University Press.
- Naji, A. B. (2006). *The Management of Savagery: The Most Critical Stage Through Which the Umma Will Pass*, William McCants, trans., John M. Olin Institute for Strategic Studies, Harvard University.
- National Research Council (2002). *Discouraging Terrorism: Some Implications of 9/11*, Washington, D.C.: National Academies Press.
- National Research Council (2009). *Evaluating Testing, Costs, and Benefits of Advanced Spectroscopic Portals for Screening Cargo at Ports of Entry: Interim Report (Abbreviated Version)*, Washington, D.C.: National Academies Press.
- Neu, C. R. (2009). *Is It Time to Rethink U.S. Entry and Exit Processes?* Santa Monica, Calif.: RAND Corporation, OP-235-RC. As of November 3, 2009:
http://www.rand.org/pubs/occasional_papers/OP235/
- Office of National Drug Control Policy (2001). "Measuring the Deterrent Effect of Enforcement Operations on Drug Smuggling, 1991–1999," August 2001.
- Perliger, A., Pedahzur, A. (2006). "Coping with Suicide Attacks: Lessons from Israel," *Public Money and Management*, November 2006, pp. 281–286.
- Phillips, P. J. (2009). "Applying Modern Portfolio Theory to the Analysis of Terrorism: Computing the Set of Attack Method Combinations from Which the Rational Terrorist Group Will Choose in Order to Maximize Injuries and Fatalities," *Defence and Peace Economics*, Vol. 20, pp. 193–213.
- Pita, J., Jain, M., Ordonez, F., Portway, C., Tambe, M., Western, C., Paruchuri, P., Kraus, S. (2009). "Using Game Theory for Los Angeles Airport Security," *AI Magazine*, Vol. 30, pp. 43–57.
- Powell, R. (2007). "Defending Against Terrorist Attacks with Limited Resources," *American Political Science Review*, Vol. 101, pp. 527–541.
- Quillen, C. (2007). "Three Explanations for al-Qaeda's Lack of a CBRN Attack," *Terrorism Monitor*, Vol. 5, No. 3.
- Radlauer, D. (2006). "Rational Choice Deterrence and Israeli Counter-Terrorism," *Lecture Notes in Computer Science*, No. 3975, ISI 2006, pp. 609–614.
- Roberts, B. (2007). "Deterrence and WMD Terrorism: Calibrating Its Potential Contributions to Risk Reduction," Alexandria, Va.: Institute for Defense Analyses.

- Sandler, T., Tschirhart, J. T., Cauley, J. (1983). "A Theoretical Analysis of Transnational Terrorism," *The American Political Science Review*, Vol. 77, pp. 36–54.
- Schelling, T. (1960), *The Strategy of Conflict*, Cambridge, Mass.: Harvard University Press.
- Schmitt, E., Shanker, T. (2006). "U.S. Adapts Cold-War Idea to Fight Terrorists," *The New York Times*, March 18, 2006.
- Stevens, D., Schell, T. L., Hamilton, T., Mesic, R., Brown, M. S., Chan, E. W., Eisman, M., Larson, E. V., Schaffer, M., Newsome, B., Gibson, J., Harris, E. (2004). *Near-Term Options for Improving Security at Los Angeles International Airport*, Santa Monica, Calif.: RAND Corporation, DB-468-1-LAWA. As of November 3, 2009:
http://www.rand.org/pubs/documented_briefings/DB468-1/
- Stewart, M. G., Mueller, J. (2008). "A Risk and Cost-Benefit Assessment of United States Aviation Security Measures," *Journal of Transportation Security*, Vol. 1, pp. 143–159.
- Stone, J. (2009). "Al Qaeda, Deterrence, and Weapons of Mass Destruction," *Studies in Conflict & Terrorism*, Vol. 32, No. 9, pp. 763–775.
- Sunstein, C. (2003). "Terrorism and Probability Neglect," *Journal of Risk and Uncertainty*, Vol. 26, pp. 121–136.
- Trager, R. F., Zagorcheva, D. P. (2005–2006). "Deterring Terrorism: It Can Be Done," *International Security*, Vol. 30, pp. 87–123.
- Transportation Research Board (2002). "Deterrence, Protection, and Preparation: The New Transportation Security Imperative—Special Report 270," Washington, D.C.: National Academies Press.
- Urban, M. (1992). *Big Boys' Rules: The Secret Struggle Against the IRA*, London: Faber & Faber.
- U.S. Office of Homeland Security (2002). *National Strategy for Homeland Security*.
- Veness, D. (1999). "Low Intensity and High Impact Conflict," *Terrorism and Political Violence*, Winter 1999, pp. 8–14.
- Willis, H. H., Morral, A. R., Kelly, T. K., Medby, J. J. (2005). *Estimating Terrorism Risk*, Santa Monica, Calif.: RAND Corporation, MG-388-RC. As of November 3, 2009:
<http://www.rand.org/pubs/monographs/MG388/>
- Wilson, J. R., Jackson, B. A., Eisman, M., Steinberg, P., Riley, K. J. (2007). *Securing America's Passenger-Rail Systems*, Santa Monica, Calif.: RAND Corporation, MG-705-NIJ. As of November 3, 2009:
<http://www.rand.org/pubs/monographs/MG705/>
- Zhuang, J., Bier, V. M. (2007). "Balancing Terrorism and Natural Disasters—Defensive Strategy with Endogenous Attacker Effort," *Operations Research*, Vol. 55, pp. 976–991.
- Zhuang, J., Bier, V. M. (2009). "Secrecy and Deception at Equilibrium, with Applications to Anti-Terrorism Resource Allocation," *Defence and Peace Economics*, forthcoming.
- Zhuang, J., Bier, V. M., Alagoz, O. (2009). "Modeling Secrecy and Deception in a Multiple-Period Attacker-Defender Signaling Game," *European Journal of Operational Research*, forthcoming.